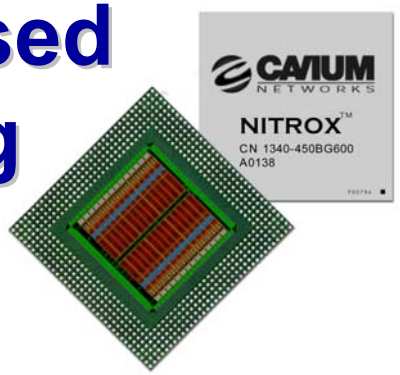
PlatformConference

Direction • Design • Perspective • Analysis

HyperTransport™ Based Security Processing



Jeff Twombly

VP Sales and Marketing

Cavium Networks

jeff.twombly@cavium.com

CAVIUM NETWORKS

January 23-24, 2002

Internet Security Applications

Web-Security

- **Servers**
  - Web Servers hosting applications using SSL protocol
  - Signature verification for B2B exchange protocol
  - Remote Access Servers with SSL for secure mail
- **Web Switches and Appliances**
  - SSL/TLS Termination and Content switching
  - Content Aware Server Load Balancers
  - SSL Proxy Servers
- **Wireless WAP gateways**

Network Security

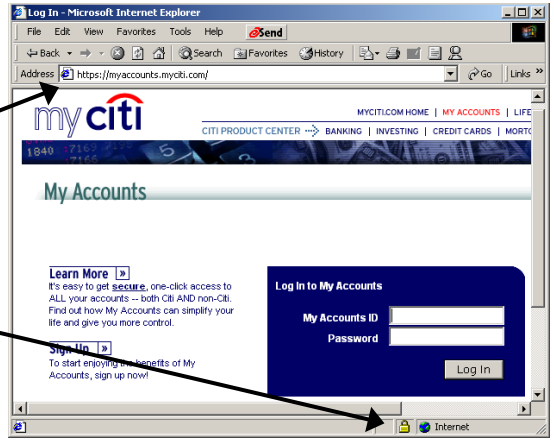
- **Network Access Gateways**
  - Firewalls and Dedicated VPN Gateways
- **Network Infrastructure Devices**
  - Switches and Routers
- **Network Storage Devices**
  - Storage Area Network systems (SAN and NAS)

Major Internet Security Protocols

Web based security uses

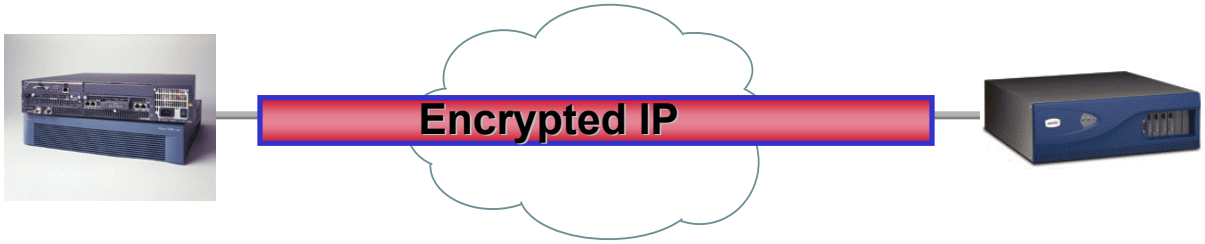
SSL Protocol

https:// and the yellow lock indicate SSL being used



Clicking on the yellow lock opens the certificate information

IP based security uses **IPsec Protocol** and is also referred to VPN



Between host or gateways

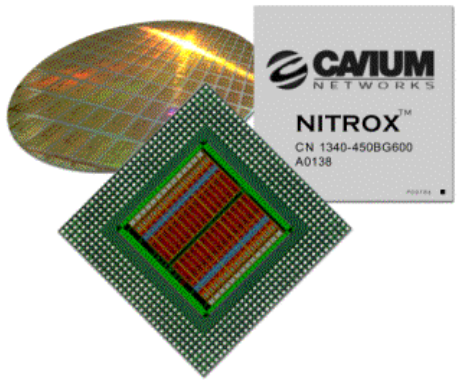
Why does security slow down the system?

- Security involves
  - Ability to verify identity (Authentication)
    - Up to 2048 bit modular arithmetic
  - Ability to cipher/decipher (Confidentiality)
    - Matrix arithmetic and numerous table look ups
  - Ability to maintain data integrity (Integrity)
    - More than 512 32-bit additions per 64-byte processed block
  - Ability to establish identity (Non-repudiation)
    - Up to 2048 bit modular arithmetic

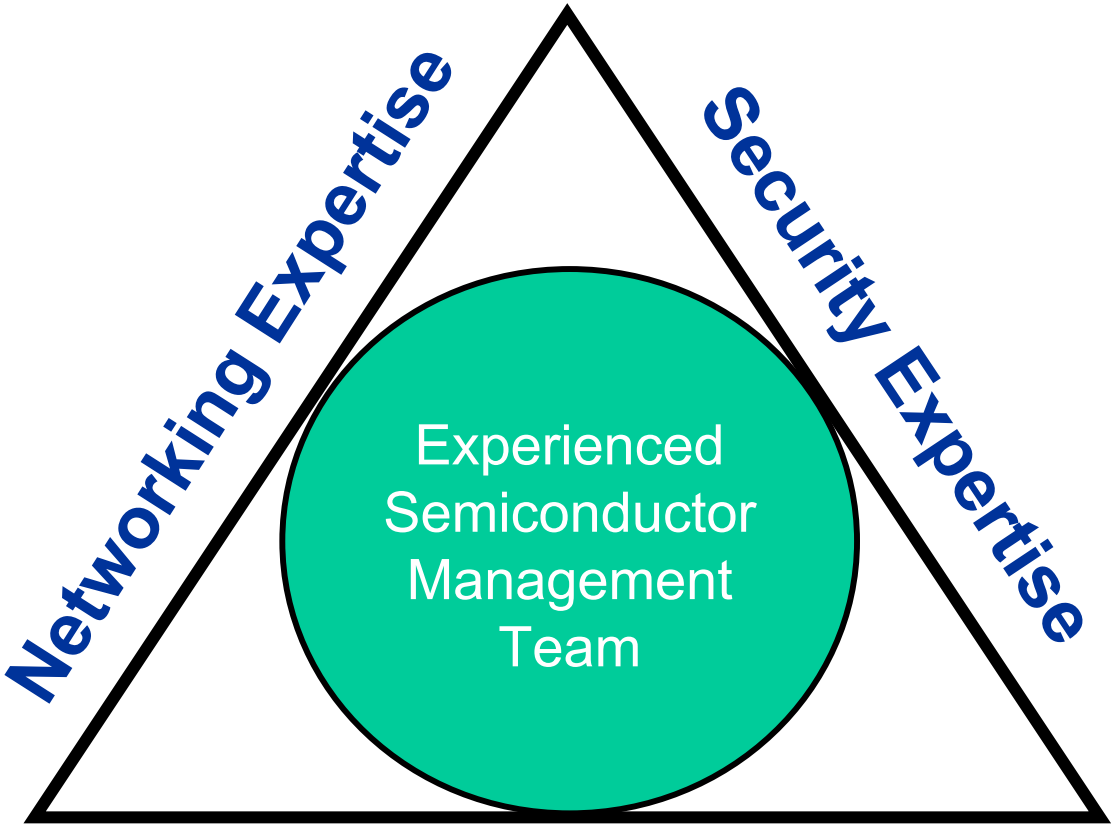
Security is VERY compute-intensive!!!

Mission

"To enable corporations to leverage the economic potential of the public internet by providing wire-speed protocol aware and packet aware security solutions that dramatically reduce the cost and complexity of deploying security"



World Class Team



World Class Custom Processor Design Team

Technical Advisory Board

- Paul Kocher
  - Co-inventor of SSL
- Stephen Kent
  - Co-inventor of IPsec
- Richard Seifert
  - Implemented the 1st Commercial 10Mbps Ethernet System

Problem's with Existing Internet Security Solutions

- Chip performance is low
- Resulting "system-level" performance is low
- Low performance busing --- PCI
- Limited scalability and programmability

Introducing

NITROX™

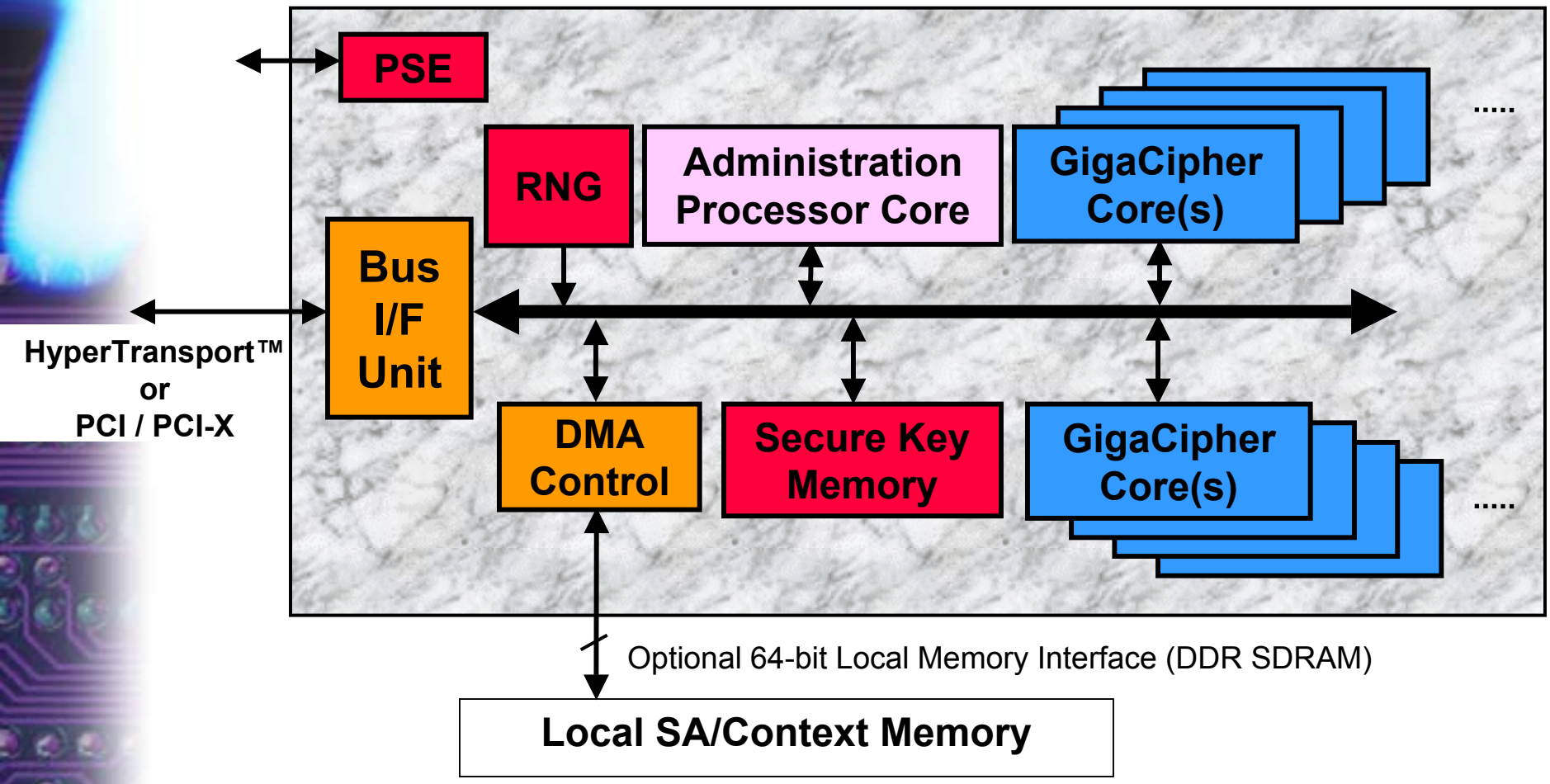
3rd Generation Security Macro Processor

" **A** Scalable, Programmable, High Performance **Processor architecture built from the ground up for** both **network and e-commerce security that can win on its** sheer performance **metrics in high performance applications and can win on** features, cost and power consumption **in lower performance applications** "

NITROX™ - Security on a chip

- **Bulk Data Encryption**
  - DES, 3DES, ARC4, AES
  - MD5, SHA-1, MAC-MD5/SHA-1, HMAC-MD5/SHA-1
- **Session Establishment**
  - RSA (2048 w/o CRT), Diffie-Hellman
  - Full SSL Handshakes (CPS)
  - IKE Acceleration
- **SSL & TLS Record Processing**
- **Packet Processing**
  - IPSEC (AH, ESP, Tunnel, Transport)
- **On-Chip Random Number Generator (RNG)**

NITROX™ - Single Chip Soulution



NITROX™ - Performance Highlights

- **Highest Chip Performance**
  - **1G to 5G** symmetric bandwidth (encryption + hashing)
  - **10K - > 50K** 1024-bit RSA ops/sec
  - **10K - > 40K** Full SSL Handshakes (CPS)
  - **10K - > 40K** Diffie-Hellman ops/sec

NITROX™ - HyperTransport™ Security

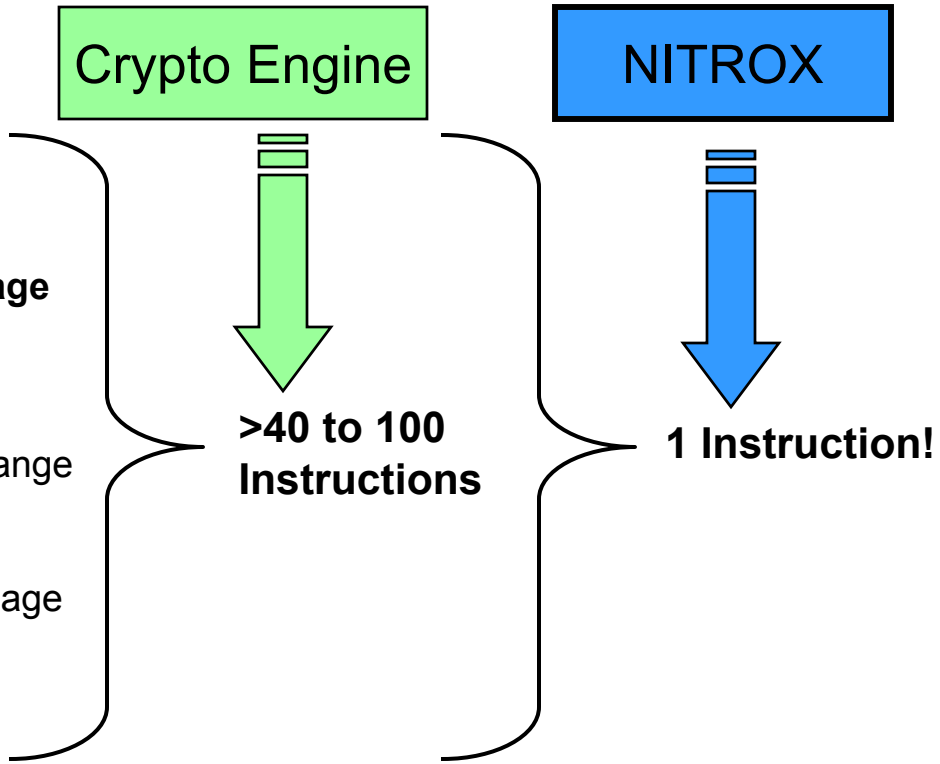
- **First HyperTransport based Single Chip Security Solution**
- **Highest System Performance**
  - Macro instructions
    - Maximize efficiency of the host CPU/NPU and the I/O Bus
  - Dynamic Resource Allocation
    - Allows for balanced & adaptive architectures to be deployed
- **Programmable**
  - Microcode engines = upgradeability
- **Scalable**
  - Various core/frequency options
  - Enables wide range of performance/price points

Macro Processing Benefits

Full SSL / TLS Handshake

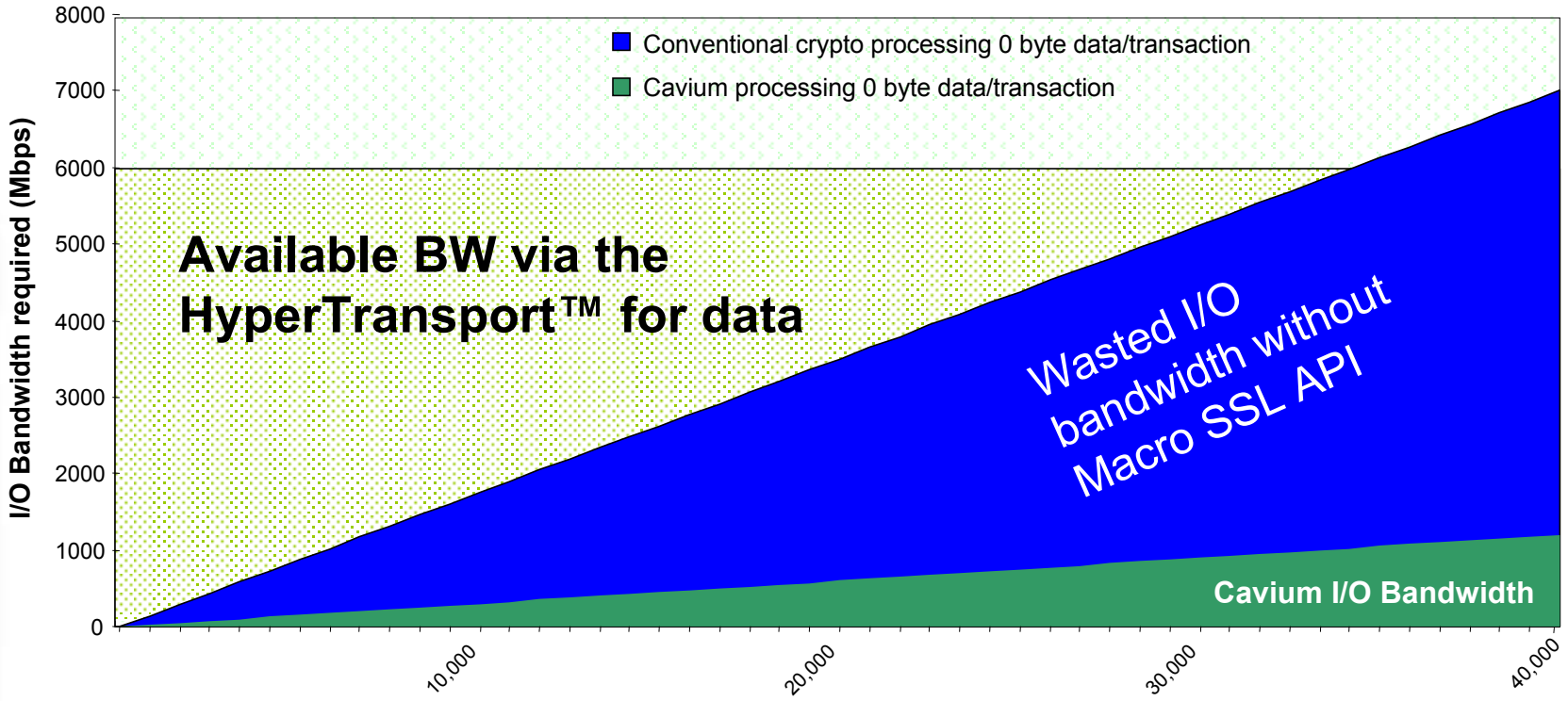
Client Hello & Server Response messages
- Partial Handshake Hash of Client Hello
- Server Responses

Client Key Exchange & Server Finish Message
- *Private Key Modular Exponentiation (RSA)*
- Master Secret
- Key material generation
- Partial Handshake Hashes of client key exchange
- Decrypt client finish message for verification
- Create Client finish locally for verification
- Partial Hashes to include client finished message
- Create server finish message
- Encrypt and Authenticate (MAC)
- Partial Hashes for Server Finish

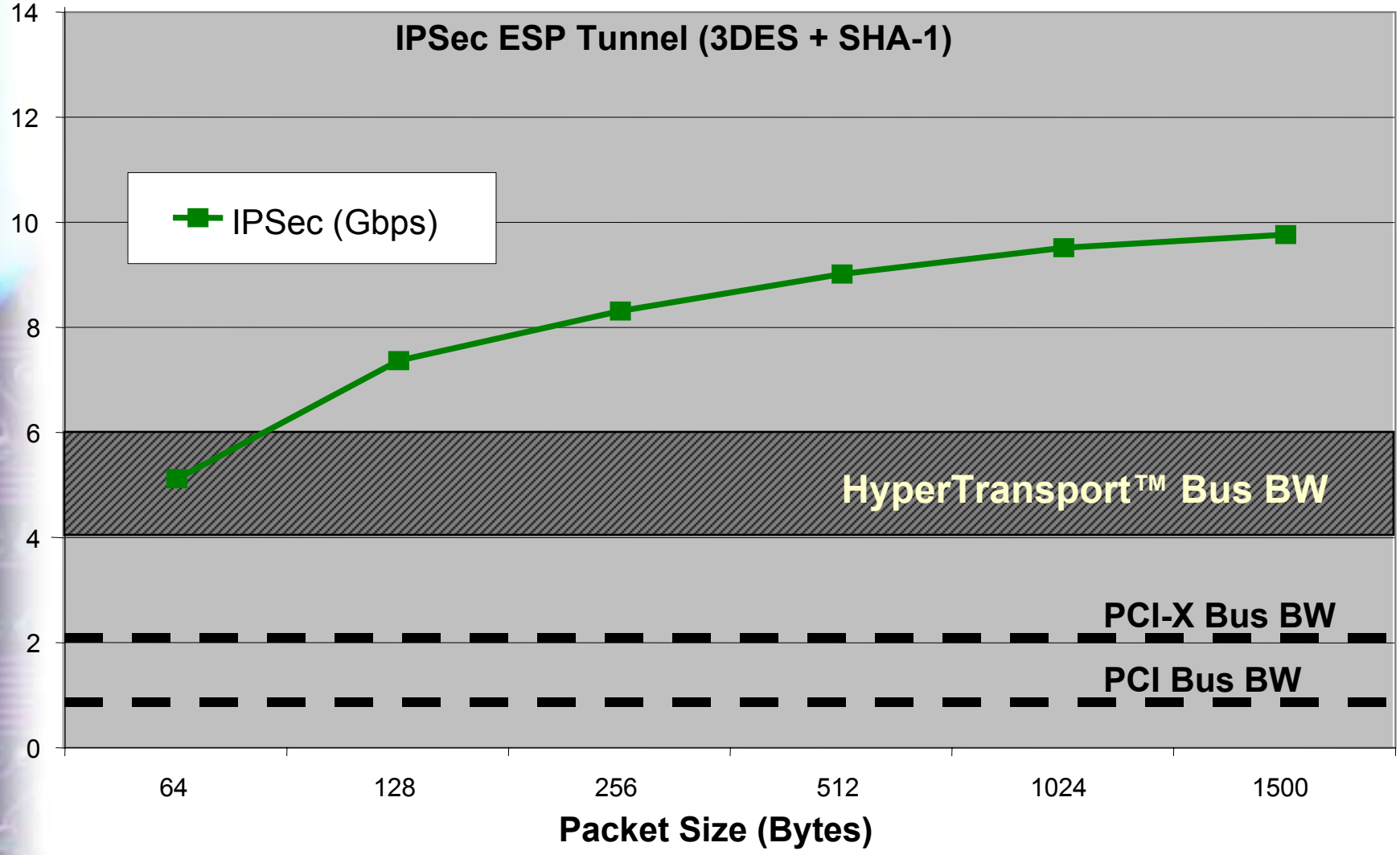


Lowest CPU overhead and optimized bus performance

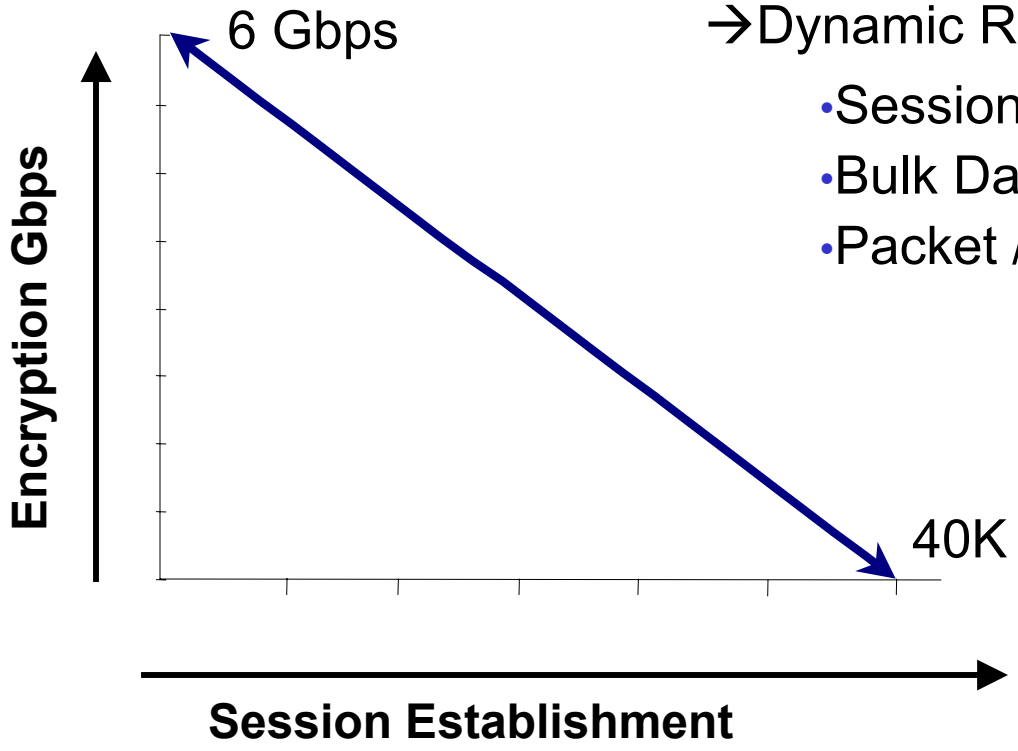
Macro Processing Benefits Combined with High Performance HyperTransport™ I/O



IPsec Packet Processing Performance



Adaptive Processing

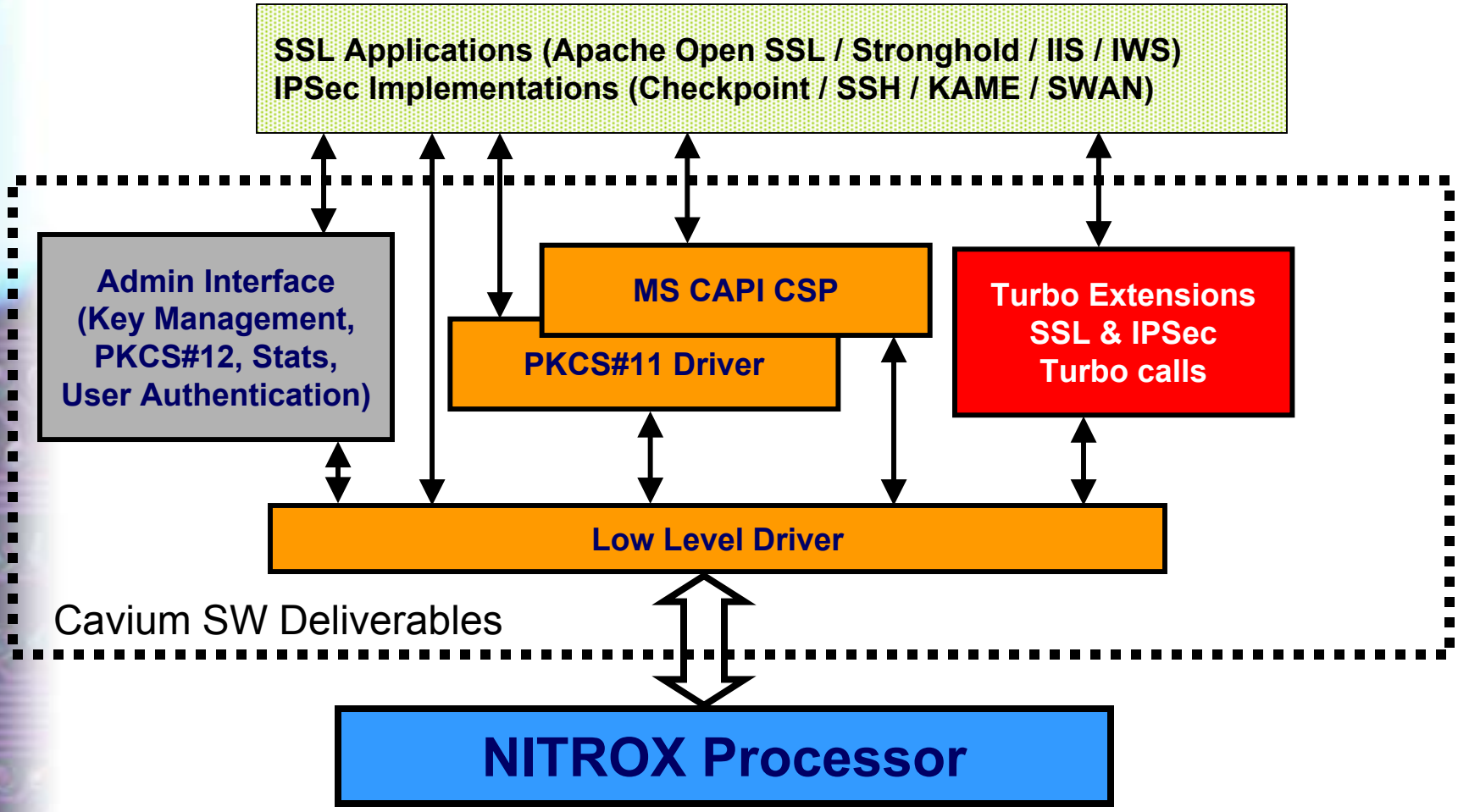


→Dynamic Resource Allocation

- Session Establishment
- Bulk Data Encryption
- Packet / Record Processing

1) Adjusts to Amazon.com or Schwab.com type loads
2) Ideal for rapid main mode tunnel establishment (or fail-over)

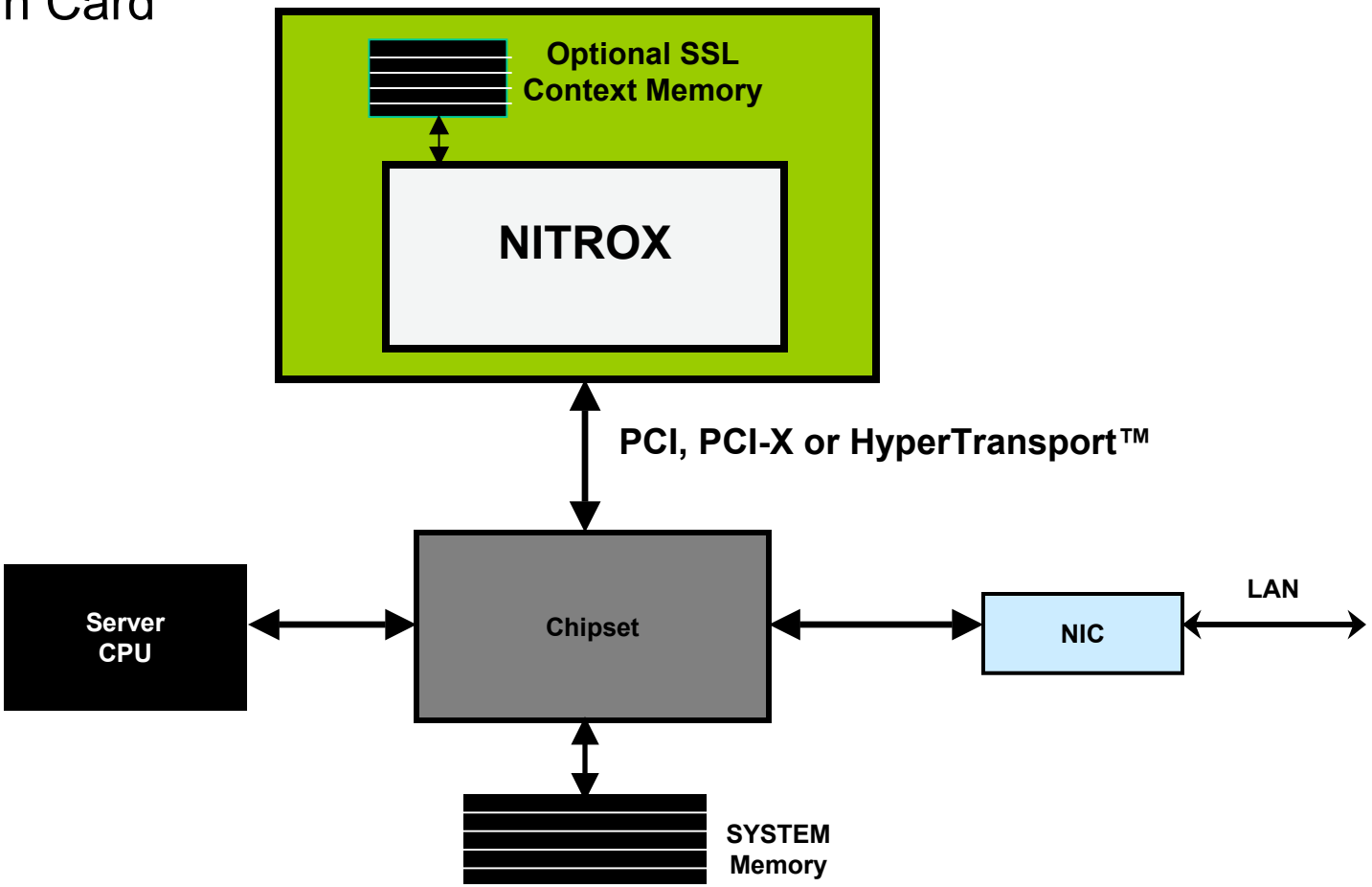
Software Interface to NITROX™ Processor



SDK Available NOW!

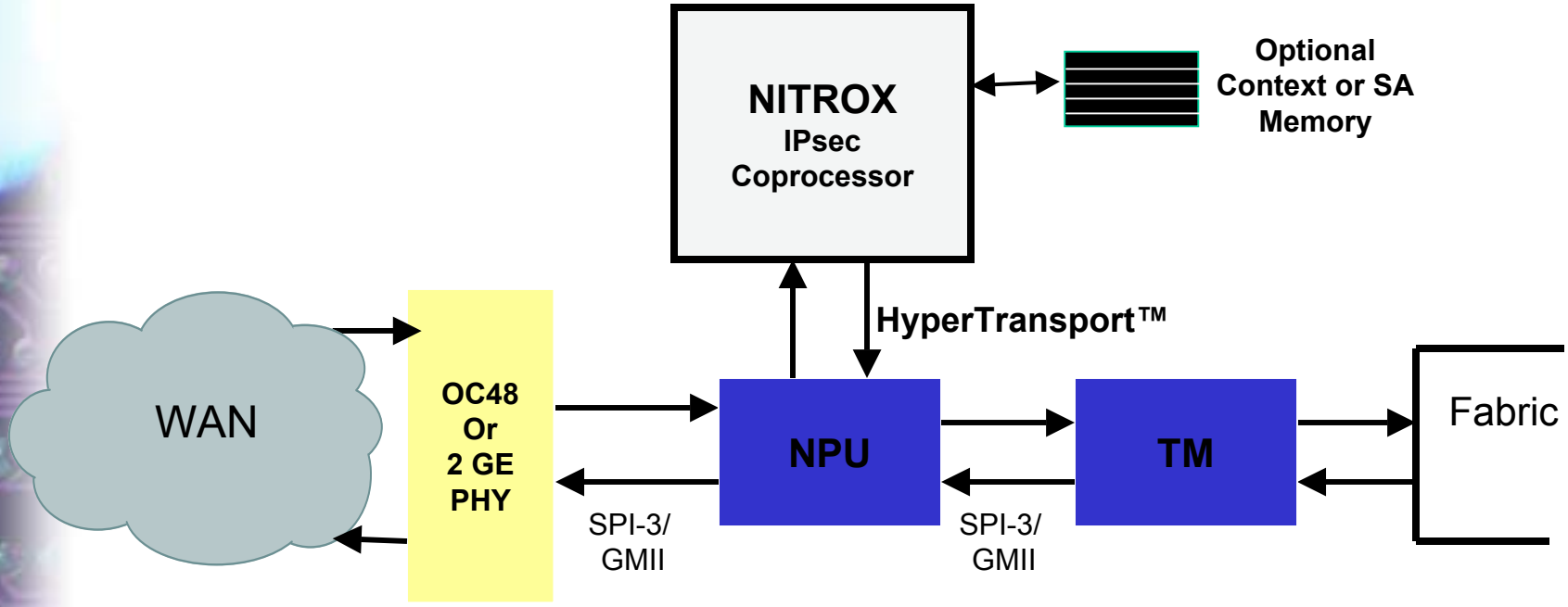
SSL Web Server Applications

Add In Card

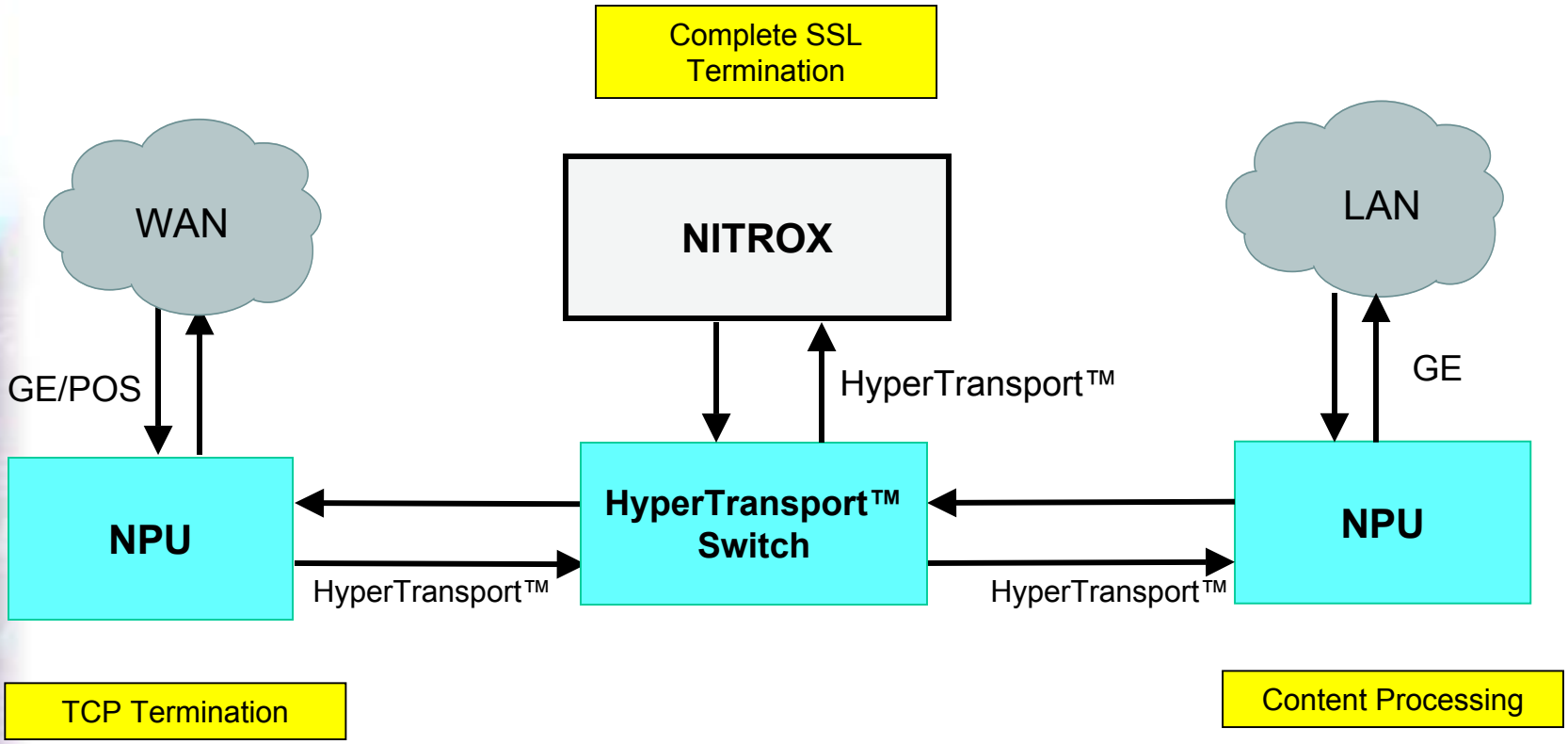


Edge Router Application using NITROX™

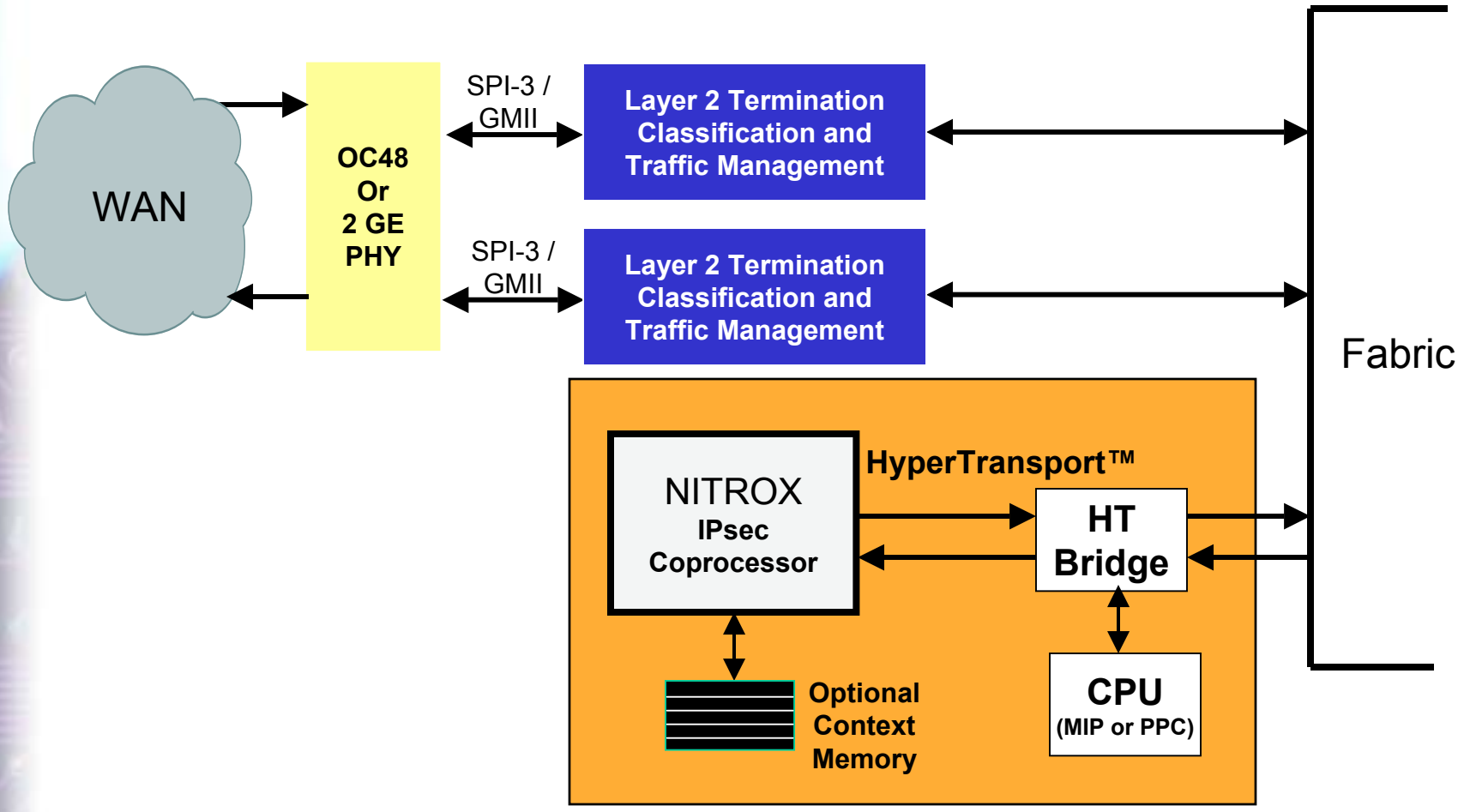
Line Card application



High End SSL Based Secure Content Processing



NITROX™ in a Service Card Application



Summary

- ✓Worlds 1st Security Macro processor
- ✓Single Chip HyperTransport™ Security Solution
- ✓Programmable
- ✓Highest Chip Performance
- ✓Highest System Performance
- ✓Scalability
- ✓Highest level of security & management features
- ✓Custom CPU Design (Lowest Cost & Power)